Homeland Security

THE NATIONAL CYBERSECURITY WORKFORCE FRAMEWORK

USER GUIDE–

COLLEGE (ACADEMIC INSTITUTIONS and EDUCATORS)

Workforce Framework User Guide

Welcome to the User Guide!

The Workforce Framework helps **Colleges** (Academic Institutions/Educator) create degree programs that are aligned to jobs.

The National Initiative for Cybersecurity Education (NICE) developed the National Cybersecurity Workforce Framework to categorize and define cybersecurity work.

When degrees, jobs, training and certifications are aligned to the Workforce Framework...
Colleges & Training Vendors can create programs that are aligned to jobs
Students will graduate with knowledge and skills that employers need
Employers can recruit from a larger pool of more qualified candidates
Employees will have a better defined career path and opportunities
Policy Makers can set standards to evolve the field

Workforce Framework User Guide

What’s in this User Guide?

This guide was created to help you and your organization use the Workforce Framework. As you navigate through the guide, you will find:

- A Workforce Framework Overview.
- Benefits of implementing the Workforce Framework within your company/organization.
- Recommended steps for implementation.
- Useful tools and links that will help you promote and use the Workforce Framework.

The National Cybersecurity Workforce Framework

Led by the Department of Homeland Security (DHS), the National Initiative for Cybersecurity Education (NICE) raises public awareness, provides a foundation for the recruitment, training, and retention of cybersecurity professionals, and promotes cybersecurity education. The Workforce Framework (in support of the "Evolve the Field" goal) is a national resource providing employers, educators, trainers, and policy makers a common language for describing cybersecurity work.

The Workforce Framework contains cybersecurity Specialty Areas, knowledge, skills, and abilities (KSAs), tasks, and sample job titles. It has been updated to reflect the evolving cybersecurity field and incorporate diverse viewpoints across government, industry, and academia. Explore the Workforce Framework at the National Initiative for Cybersecurity Careers and Studies (NICCS™) website.

The Workforce Framework is:

A Blueprint

- Describes and categorizes cybersecurity work.
- Identifies sample job titles, tasks, and knowledge, skills, and abilities (KSAs).

A Tool

- Provides a foundation organizations can use to develop position descriptions, competency models, and training.

A Collaboration

- Incorporates inputs from industry, academia, and government.
- Addresses the nation's need to identify, qualify, and develop the cybersecurity workforce.

Using the Workforce Framework – Academic Institutions/Educators

Having a common framework for describing cybersecurity work allows ***Academic Institutions*** to use a consistent language for outlining graduation requirements and developing academic programs (undergraduate and graduate level). Likewise, ***Educators*** can use the Workforce Framework to build and update curriculum. A common language also helps students and learners evaluate learning and internship opportunities, and gain insight about the cybersecurity knowledge and skills needed in the workplace.

Using the Workforce Framework, Academic Institutions can:

- Prepare students for a successful career by providing a common language, descriptions of cybersecurity work, and the knowledge and skills needed in the field.
- Meet the defined program criteria to become a National Center of Excellence (CAE) institution with Information Assurance/ Cyber Defense (IA/CD) designation. The IA/CD required knowledge units are aligned to the Workforce Framework.

Using the Workforce Framework, Educators can:

- Provide students with real-world activities and practical applications of the cybersecurity skills.
- Build new and update existing curriculum.

Why is the Workforce Framework Important?

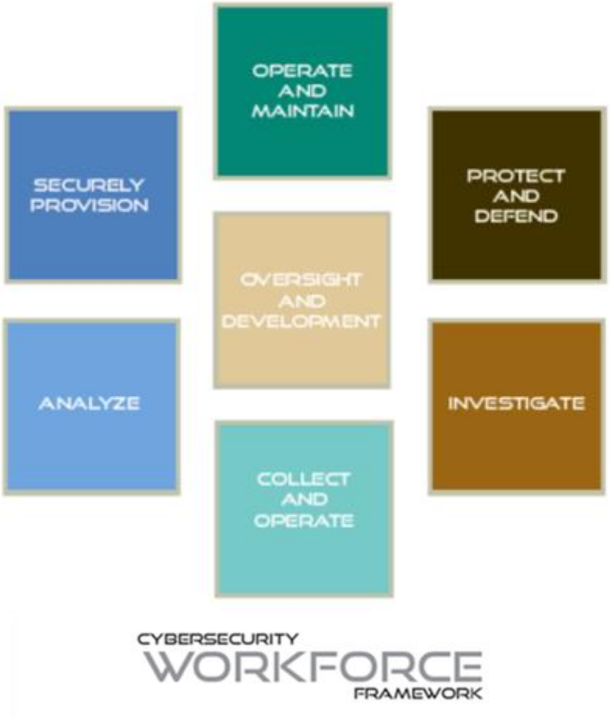
The Workforce Framework categorizes cybersecurity work and identifies cybersecurity Specialty Areas.

The Workforce Framework establishes:

- A common taxonomy and language which organizes cybersecurity work into seven Categories and more than 30 Specialty Areas.
- A baseline of tasks, Specialty Areas, and KSAs associated with cybersecurity professionals.

The Workforce Framework improves our Nation's ability to:

- Provide employers, educators, trainers, and policy makers a common language for describing cybersecurity work.
- Build and maintain the highly skilled and agile workforce needed to protect the nation.
- Coordinate and collectively address cybersecurity threats.



What are the Seven Categories?

The Workforce Framework's Categories organize Specialty Areas by grouping similar work.

Securely Provision	Specialty Areas concerned with conceptualizing, designing, and building secure IT systems.
Operate and Maintain	Specialty Areas responsible for providing the support, administration, and maintenance necessary to ensure effective and efficient IT system performance and security.
Protect and Defend	Specialty Areas responsible for identifying, analyzing, and mitigating threats to IT systems.
Investigate	Specialty Areas responsible for the investigation of cyber events or crimes which occur within IT Systems and networks.
Collect and Operate	Specialty Areas responsible for the highly specialized and largely classified collection of cybersecurity information that may be used to develop intelligence.
Analyze	Specialty Area responsible for highly specialized and largely classified review and evaluation of incoming cybersecurity information.
Oversight and Development	Specialty Areas that provide critical support so others may conduct their cybersecurity work.

What are the Specialty Areas?

Specialty Areas describe a cybersecurity work area, or function. Each Specialty Area includes related Tasks, KSAs, and sample job titles.

Securely Provision

- Technology Research and Development
- Systems Requirements Planning
- Systems Security Architecture
- Software Assurance and Security Engineering
- Systems Development
- Test and Evaluation
- Information Assurance (IA) Compliance

Analyze

- Cyber Threat Analysis
- All Source Intelligence
- Targets
- Exploitation Analysis

Collect and Operate

- Operations Planning
- Cyber Operations
- Collection Operations

Protect and Defend

- Computer Network Defense (CND) Analysis
- Vulnerability Assessment and Management
- Incident Response
- Computer Network Defense (CND) Infrastructure Support

Investigate

- Investigation
- Digital Forensics

Oversight and Development

- Strategic Planning and Policy Development
- Security Program Management (CISO)
- Information Systems Security Operations (ISSO)
- Education and Training
- Legal Advice and Advocacy

Operate and Maintain

- System Administration
- Network Services
- Customer Service and Technical Support
- Systems Security Analysis
- Data Administration
- Knowledge Management

National Initiative for Cybersecurity Careers and Studies (NICCS™)

For more information on the Workforce Framework, visit National Initiative for Cybersecurity Careers and Studies (NICCS™) website. NICCS is the one stop shop for cybersecurity careers and studies. There, you will find a wealth of information on the Workforce Framework. The site also connects you with information on:

- Cybersecurity Awareness
- Professional Certifications and Courses
- Academic and Hands-on Learning Opportunities
- Workforce Development Strategies
- Federal Cybersecurity Training Events (FedCTE)
- Federal Virtual Training Environment (FedVTE)

Visit NICCS: www.niccs.us-cert.gov/

Benefits of using the Workforce Framework

The Workforce Framework benefits **Academic Institutions and Educators** by defining cybersecurity functions and creating a common taxonomy which can be used when referring to cybersecurity work. It describes cybersecurity work irrespective of organizational structures, job titles, or other potentially individual conventions.

The Workforce Framework:

- ✓ Provides consistent language used in the field used to describe and define a cybersecurity workforce. It allows Academic Institutions and Educators to use widely accepted language and defined skills to build curriculum.
- ✓ Provides common cybersecurity roles students can learn about and explore within their academic pursuits.
- ✓ Helps distinguish educational excellence programs like the National Centers of Academic Excellence (CAE) institutions. This program promotes Information Assurance (IA) Cyber Defense (CD) educational programs which prepare students for cybersecurity careers.
- ✓ Helps Educators align lesson plans and curriculum to real-world activities and practical applications of cybersecurity skills.

National Center of Academic Excellence (CAE)

The National Security Agency (NSA) and DHS's CAE program promotes IA/CD education, training, and awareness nationwide. The program grants CAE designation to Academic Institutions (i.e., 2-year, 4-year, and graduate) providing educational excellence in fields related to IA and cybersecurity.

CAE-IA/CD applicant institutions must meet the defined program criteria and have active courses covering the mandatory knowledge units stated in the academic content requirements. Applicant institutions must also show course alignment to mandatory/optional knowledge units listed in the Knowledge Unit (KU) Alignment Worksheet. Designated institutions that continually demonstrate student completion of CAE IA/CD courses, may indicate this accreditation on student transcripts, diplomas, and other documents of merit.

To achieve a CAE IA/CD designation, institutions should,

1. Understand CAE program requirements.
2. Become familiar with the Workforce Framework (e.g., common language/taxonomy).
3. Map courses to the mandatory KUs of the IA/CD designation.
4. Apply to the CAE program.

Contact Us

To learn more about the Workforce Framework and other Cybersecurity Education and Awareness (CE&A) Programs, please contact:

Robin “Montana” Williams
Branch Chief, DHS Cybersecurity Education & Awareness
Phone: (703) 235-5169
Email: robin.williams@hq.dhs.gov

Kristina Dorville
Deputy Branch Chief, DHS Cybersecurity Education & Awareness
Phone: (703) 235-5281
Email: kristina.dorville@hq.dhs.gov